Symantec AntiVirus™ Corporate Edition

Comprehensive virus protection for enterprise workstations and network servers

Enterprise-wide virus protection is now a core business requirement due to the increasing frequency of rapidly spreading, destructive viruses. However, virus protection at the firewall and email gateway alone does not provide sufficient protection. Comprehensive virus protection at the workstation and network server tiers is needed to ensure system uptime and user productivity.

Symantec AntiVirus™ Corporate Edition provides scalable, cross-platform virus protection for workstations and network servers throughout the enterprise to ensure system uptime and user productivity.

New features in this release

- EXPANDED THREAT MANAGEMENT detects unwanted applications such as spyware and adware, identifies the source of blended threat attacks that spread via open file shares, and terminates suspect processes in memory before they cause damage.
- ENHANCED EMAIL PROTECTION prevents client systems from spreading worms via email, and also scans Internet email attachments delivered through POP3 mail clients.
- ENHANCED REMOTE USER PROTECTION AND MANAGEMENT ensures systems are in full compliance with corporate policy prior to accessing corporate network resources and allows machines not connected to the network to store and forward event data to the management server after reconnecting.

Centralized configuration and management

The Symantec System Center™ management console enables centralized configuration, deployment, policy management and reporting,* and can manage hundreds of thousands of nodes.

- CENTRALIZED MANAGEMENT CAPABILITIES enable IT administrators to manage individual users and functional groups of users and create, deploy, and lock down policies and settings. All workstation and network server settings can be locked down so users cannot change them, or administrators can configure and monitor workstations and network servers via the management console.
- AUTOMATIC VIRUS REPAIRS AND ALERTS when a virus is detected. A repair is automatically launched and an alert is broadcast to the IT administrator via the Symantec System Center console.
- FAST RESPONSE TO THREATS Administrators can force a LiveUpdate session to occur immediately on single or multiple clients, minimizing response time to fast-spreading threats. For even faster, automated response, push technology is incorporated into a management server associated with the Symantec System Center. The management server can be scheduled to automatically retrieve virus content updates from Symantec or from a central LiveUpdate Server. It then pushes these updates to secondary servers that in turn push the updates to client systems.
- NETWORK AUDIT FEATURE enables administrators to identify which nodes are unprotected and vulnerable to virus attack, as well as those protected by Symantec AntiVirus, McAfee® VirusScan,® Trend Micro™ Office Scan,™ Computer Associates,® or other third-party antivirus products.

* Available at additional cost.

KEY POINTS

- Advanced, enterprise-wide virus protection and monitoring from a single console
- **NEW!** Expanded Threat Detection and Threat Categorization recognizes unwanted applications such as spyware and adware
- **NEW!** Threat Tracer identifies the source of blended threat attacks that spread via open file shares
- **NEW!** Outbound email worm heuristics prevent client systems from spreading worms via email
- **NEW!** Internet Email Attachment Scanning of incoming message body text and attachments delivered through POP3 mail clients
- **NEW!** Symantec VPN Sentry ensures systems are in full compliance with corporate policy prior to accessing corporate network resources
- **NEW!** Store and Forward Event Data ensures that machines not connected to the network store and forward event data to the management server after reconnecting
- **NEW!** In-Memory Scanning detects threats and can terminate suspect processes in memory before they can do damage
- Centralized network auditing identifies unprotected nodes, as well as those protected by Symantec AntiVirus™ Corporate Edition and select third-party security products
- Backed by Symantec™ Security Response, the world's leading Internet security research and support organization

- COMMON DISTRIBUTION AND UPDATING MECHANISM via the Symantec System Center™ management console enables centralized deployment of virus definitions and product updates to multi-platform workstations and network servers, reducing overhead and management of virus protection updates across the enterprise.
- THREAT TRACER identifies the source of blended threat attacks, such as Code Red and Nimda, which spread via open file shares.
- MOVE CLIENTS BETWEEN SERVERS The central management console can now drag-and-drop clients from one physical parent server to another.
- LOGICAL GROUP MANAGEMENT Administrators can create and manage logical groupings of clients and servers within server groups, or multiple logical groups from a single parent server. This is especially useful for organizations that need to handle similar functional entities (such as departments or business units) in the same way, reducing the infrastructure cost.
- PRODUCT PATCHING allows administrators to quickly deploy bug security fixes and new versions at minimal cost.
- STORE AND FORWARD EVENT DATA enables the client to store event data if it cannot connect to the management server. The data is forwarded to the management server the next time the client connects, to ensure that critical event data is always available for alerting, logging and reporting.*
- EASE OF MIGRATION Installation tool checks for legacy versions of Norton AntiVirus™ Corporate Edition 7.x and above. If found, the install will retain the user settings, remove the previous technology from the client or server, and install the new solution.
- SECURITY SOFTWARE UNINSTALLER minimizes the cost of switching from a third-party antivirus product to Symantec AntiVirus Corporate Edition.
- SILENT OR INACTIVE INSTALL OPTIONS for installation flexibility to client machines for behind the scenes (in silent mode), or full user interaction.
- LIMITED OR FULL USER INTERFACE with password protection allows the administrator to determine if a user will be granted full or limited access to the user interface.

Award-winning virus protection

Award-winning Symantec antivirus technologies detect and protect against viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats. A reduced virus definition file size and multi-threaded server rollout speed update distribution, and growing traffic volumes are accommodated with automatic load balancing across multiple servers, to ensure highly scalable virus protection.

- EXPANDED THREAT DETECTION AND THREAT CATEGORIZATION extends the ability to detect both viral and non-viral threats. Expanded threat detection recognizes unauthorized programs that can compromise the security of the system (e.g., viruses, worms, and Trojans), the privacy of client data (e.g., spyware, trackware, and adware), or that can be used with malicious intent (e.g., dialers, joke programs, remote access and hack tools).

- BEHAVIOR BLOCKING Outbound email worm heuristics detect malicious applications to prevent client systems from spreading worms via email (such as SOBIG.F).
- APPLICATION SECURITY/TAMPER RESISTANCE logs any attempts of unauthorized registry changes. This feature also adds authentication to policy and definition updates delivered from the Symantec System Center to the client. The real-time virus scanning technology is automatically enabled if turned off for a considerable amount of time.
- COMMON SCAN ENGINE enables a single virus definition to be deployed to workstations and servers regardless of supported platform or language.
- NAVEX™ extensible scan engine technology updates virus definitions and scan engines without having to redeploy the software or reboot the system.
- HIGH-PERFORMANCE SCANNING places minimal resource demands on the existing network infrastructure. It scans compressed files 50 percent faster than previous versions by decompressing files in memory.
- UNKNOWN VIRUS DETECTION BloodHound™ heuristic detection technology identifies unknown viruses by detecting virus-like behavior. Bloodhound can detect up to 90 percent of new macro viruses and up to 80 percent of new and unknown executable file viruses, including malicious mobile code.
- CENTRAL QUARANTINE allows administrators to redirect all irreparable, virus-infected files to a safe area on a centralized server for further inspection. This feature strips sensitive, proprietary data from macro virus-infected files, removes the viruses from the main computing environment, and prevents them from spreading throughout the organization.
- AUTOMATED RESPONSE The Digital Immune System™ automates the submission of potential virus threats and automatically delivers cures to the problem machine or the entire enterprise.
- EMAIL SCANNING FOR MICROSOFT® EXCHANGE AND DOMINO™ SERVER Optional components provide the ability to scan incoming email and attachments from Microsoft Exchange and Lotus Domino servers, to prevent unnecessary usage of mail data stores.
- SCAN DELAY AND PRIORITY OPTIONS allow the user to delay an administrator-scheduled scan and to adjust the priority of a scan to only scan at idle mode.
- COMPRESSED FILE SUPPORT has been enhanced to support today's most popular formats, including:

ArcManager
Cabinet Files
Symantec Ghost Image
BinHex
LHA (LZH) Files
Multipurpose Internet Mail Extensions
RAR Files
TAR Archives
UUE Archives
ARJ Files
Executable Files
GNU Compressed Format
Hyper-Text Transfer Protocol
Microsoft Compressed Files
OLESS Containers
Rich Text Format
MS-TNEF Attachment Files
Zip Archive Files

Increased remote user management and protection

- INTERNET EMAIL ATTACHMENT SCANNING Virus scanning of incoming email body text and attachments delivered through POP3 mail clients like Microsoft® Outlook®, Microsoft Outlook Express, Eudora® and Netscape Mail .

- SYMANTEC VPN SENTRY ensures mobile and remote systems connecting to corporate resources via VPN are compliant with security policies. Specifically, it checks to ensure that antivirus software is installed and real-time protection is turned on; virus definitions are up-to-date; and the client firewall is installed, enabled, and follows appropriate policy.
- ROAMING SUPPORT allows the client to "roam" and collect virus definitions and policies from the closest parent server, enabling maximum bandwidth usage.
- BATTERY CHECK determines whether or not a laptop is running on batteries so a scheduled scan can be deferred until the laptop is using AC power.

For more information about Symantec AntiVirus Corporate Edition 9.0,
visit http://enterprisesecurity.symantec.com

VIRUS PROTECTION IS A KEY COMPONENT OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.

SYSTEM REQUIREMENTS

SYMANTEC ANTIVIRUS™ CORPORATE EDITION 9.0

SYMANTEC ANTIVIRUS MANAGEMENT SERVER – 32-BIT WINDOWS

- Windows® XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/ Terminal Server Edition SP6a
- 64 MB RAM
- 111 MB available disk space
- 15 MB available disk space for AMS2 server files (If you choose to install AMS2 Server)
- Microsoft Internet Explorer 4.01 or later

SYMANTEC ANTIVIRUS MANAGEMENT SERVER - NETWARE

- NetWare 5.1 SP3 or higher/6.0 SP1 or higher
- 15 MB RAM for Symantec AntiVirus NLMs
- 116 MB available disk space
- 20 MB available disk space for AMS2 server files (If you choose to install AMS2 Server)

SYMANTEC ANTIVIRUS FOR 32-BIT WINDOWS CLIENTS

- Windows 98/98 SE/Me Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/ Terminal/Terminal Server Edition SP6a
- 32 MB RAM
- 55 MB available disk space
- Microsoft Internet Explorer 4.01 or later
- Intel Pentium processor at 150 MHz (Pentium II or higher recommended)

SYMANTEC ANTIVIRUS FOR 64-BIT WINDOWS CLIENTS

- Windows XP 64-Bit Edition Version 2003/Server 2003 Enterprise/Datacenter 64-Bit Editions
- Intel® Itanium 2 processor
- 64 MB RAM
- 70 MB available disk space

SYMANTEC SYSTEM CENTER

- Windows XP Professional/2000 Professional/Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/ Terminal Server Edition SP6a
- Microsoft Management Console 1.2 (If MMC is not already installed, you will need 3 MB of available disk space - 10 MB during installation)
- 32 MB RAM
- 36 MB available disk space
- Microsoft Internet Explorer 5.5 SP2 or later

SYMANTEC SYSTEM CENTER SNAP-INS

Alert Management System Console

- 24 MB available disk space in addition to the Symantec System Center requirements

Symantec AntiVirus Snap-in

- 6 MB available disk space in addition to the Symantec System Center requirements

Symantec Client Firewall Snap-in

- 1 MB available disk space in addition to the Symantec System Center requirements

AV Server Rollout Tool

- 130 MB available disk space in addition to the Symantec System Center requirements

NT Client Install Tool

- 2 MB available disk space in addition to the Symantec System Center requirements

QUARANTINE CONSOLE

- Windows XP Professional/2000 Professional/Server/Advanced Server/NT 4.0 Workstation
- Microsoft Management Console 1.2 (If MMC is not already installed, you will need 3 MB of available disk space - 10 MB during installation)
- 32 MB RAM
- 35 MB available disk space
- Microsoft Internet Explorer 5.5 SP2 or later

QUARANTINE SERVER

- Windows XP Professional/2000 Professional/ Server/Advanced Server/Server 2003 Web/Standard/Enterprise/Datacenter Edition/NT 4.0 Workstation/Server/Terminal/Terminal Server Edition SP6a
- 64 MB RAM
- 40 MB available disk space
- Minimum swap file size of 250 MB
- 500 MB - 4 GB disk space recommended for quarantined items
- Microsoft Internet Explorer 5.5 SP2 or later

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. LiveUpdate, and NAVEX are trademarks of Symantec Corporation. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States and other countries. All other brands and products are trademarks of their respective holder/s. Copyright © 2004 Symantec Corporation. All rights reserved. Printed in the U.S.A. 04/04 All product information is subject to change.
10270835

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product Information
In the U.S., call toll-free
800.745.6054

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.